Cyber Security Guide – KMU

Wir zeigen Ihnen den Weg durch den digitalen Dschungel

Über die Baloise Digital Scouts

Das Digital Scouts-Team von Baloise besteht aus motivierten und interessierten Mitarbeitenden. Als Botschafter der Digitalisierung wollen wir unseren Mitmenschen dabei helfen, den Weg durch den digitalen Dschungel zu finden. Die Organisation der Baloise Digital Scouts entstand aus einer Zusammenarbeit der Bereiche Group IT und Corporate Communications.

Die Baloise Digital Scouts leisten im Rahmen der Corporate Social Responsibility von Baloise einen freiwilligen Beitrag, da die Bedürfnisse der Gesellschaft weiter gehen als der Bezug von Sicherheitsleistungen. Baloise-Mitarbeitende verfügen über ein breites Know-how. Dieses wird über die geschäftsrelevanten Dienstleistungen hinaus der Gesellschaft zur Verfügung gestellt.

Sind Sie an einer Infoveranstaltung über Cyber Security interessiert?

Kontaktieren Sie uns per E-Mail:
scouts@baloise.com

Über diese Broschüre

Diese Broschüre soll KMUs dabei helfen, ihre Mitarbeitenden über die Gefahren und Risiken beim alltäglichen Gebrauch des Internets am Arbeitsplatz und zu Hause zu informieren. Weiter erklärt sie die Grundlagen der Cyber Security und zeigt präventive Richtlinien zur Verhinderung von Cyber-Vorfällen auf.

Cyber Security-Risiken existieren in vielen Formen und können unterschiedlich grosse und verheerende Schäden anrichten. Der Mensch verursacht nach wie vor die meisten Sicherheitsvorfälle in einem Unternehmen. Durch klares Verständnis der Risiken und der Konsequenzen des eigenen Handelns kann dieses Risiko jedoch wesentlich reduziert werden.

Informationsschutz ausserhalb der Geschäftsräumlichkeiten

Social Engineering
Für viele Unternehmen gehört geschäftliches Reisen zum Alltag oder sogar zum Geschäftszweck. Es ist wichtig, dabei auch die Informationssicherheit zu bewahren und sich der Gefahren bewusst zu sein. Sei es im Zug, in der Hotel-Lobby, in einem Café oder auf der Strasse: überall können fremde Ohren mithören oder fremde Augen mitlesen und dies bei Gelegenheit zu ihrem Vorteil ausnutzen. Mitarbeitende müssen daher sensibilisiert werden, auch ausserhalb der Geschäftsräumlichkeiten für den Schutz von Informationen zu sorgen.

Homeoffice
Mitarbeitende, die zuhause arbeiten, müssen sich bewusst sein, dass sie die geschäftlichen Daten genauso gut schützen wie im Büro. Dazu gehört, geschäftliche und private Daten nicht zu mischen. Besser sind daher getrennte Geräte. Falls sie jedoch die eigenen (privaten) Geräte verwenden dürfen, sollten sie auch mit den nötigen Informationen zum Schutz der Daten versorgt werden. Regeln Sie daher mindestens folgende Punkte:

- Durchführung von regelmässigen Updates
- Verwendung von HTTPS-Seiten und VPN für eine sichere Verbindung
- Sichere Entsorgung von sensiblen schriftlichen Informationen (nicht im Altpapier)
- Verwendung von Hintergrundbildern und Teilen von Inhalten bei Video-Konferenzen
- Durchführung von Backups
- Meldung von aussergewöhnlichen Auffälligkeiten

Im öffentlichen Raum
Sobald man in der Öffentlichkeit arbeitet, sei es bei einem Geschäftsessen im Restaurant oder auf dem Weg nach Hause im Zug, können Gespräche mitgehört werden. Daher ist es wichtig, die Worte so zu wählen, dass Mithörende nicht auf etwas schliessen können. Ausserdem ist die Verwendung von einem Blickschutz zu empfehlen, wenn fremde Personen auf den Laptop oder das Mobiltelefon schauen können. Gewisse Gespräche sollten deshalb nur in einem geschützten Raum geführt werden. Auch besteht die Gefahr eines Diebstahls von Geräten, die kurz ausser Acht gelassen werden.

Tipps

- Sensibilisieren Sie ihre Mitarbeitenden, damit sie die Informationssicherheit auch auf Geschäftsreisen oder zuhause bewahren.
- Machen Sie Gespräche in der Öffentlichkeit sicherer, indem Sie zum Beispiel nur den ersten Buchstaben von Namen nennen oder «meine Organisation» statt den Firmennamen sagen.
- Verwenden Sie Blickschutzfolien (Privacy-Filter) und erschweren Sie so das Mitlesen durch Neugierige.

Umgang mit Passwörtern und deren Sicherheit

Passwörter sollten nicht aufgeschrieben und mit niemandem geteilt werden. Multi-Faktor-Authentifizierung ist eine gute und einfache Art, die Sicherheit eines Accounts zu steigern. Dabei wird beispielsweise beim Login nach Eingabe von Benutzernamen und Passwort ein weiterer Code aus einer Authenticator App verlangt, die Sie auf Ihrem Mobilgerät installiert haben. Es ist wichtig, dass für jeden Account verschiedene Passwörter verwendet werden, die sich auch nicht zu sehr ähneln. Wenn der Verdacht besteht, dass ein Passwort verloren oder durch einen anderen Vorfall kompromittiert wurde, muss es umgehend geändert werden. Dabei ist es wichtig, nicht nur eine Zahl oder einen Buchstaben zu ändern, sondern sich ein komplett neues Passwort auszudenken.

Passwort-Manager
Für jeden Dienst sollte man einen eigenen Account mit unterschiedlichen Passwörtern verwenden. Um das Ausdenken und Merken von neuen und bestehenden Passwörtern zu vereinfachen, gibt es sogenannte Passwort-Manager. Mit diesen Applikationen ist es möglich, ein sicheres Passwort zu generieren und dieses in Verbindung mit einem Account abzuspeichern. Die Applikation selbst wird durch ein komplexes Master-Passwort oder auf dem Smartphone auch durch Fingerprint- oder Face-ID geschützt. So muss sich der Mitarbeitende nur noch das Master-Passwort merken und kann alle anderen Passwörter einfach nachschauen.

Checkliste Passwortsicherheit
- Mindestens 12 Zeichen lang (je länger, desto sicherer)
- Klein- und Grossbuchstaben
- Zahlen und Sonderzeichen wie: !, &, %, ç, +
- Keine im Wörterbuch aufgelisteten Wörter
- Keine Buchstabenfolgen wie «abcdefgh»
- Noch nie zuvor verwendetes Passwort
- Ideal: Passwort von einem Passwortsatz

So kreieren Sie einen Passwortsatz
1. Wählen Sie einen Satz, der Ihnen problemlos einfällt.
2. Verwenden Sie alle Anfangsbuchstaben in ihrer Reihenfolge, Gross- beziehungsweise Kleinschreibung und Zahlen. Diese Abfolge von Zeichen ergibt das neue Passwort.
3. Ersetzen sie schliesslich Satzzeichen mit einem Sonderzeichen und ein sicheres und leicht zu merkendes Passwort ist erstellt.

Beispiel:
Mein Sohn ist im Februar 1994 geboren.
Er ist dieses Jahr 24 geworden!
Passwortsatz: MSiiF94g.EidJ24g!

Tipps

- Verwenden Sie Multi-Faktor-Authentifizierung auch für Ihren Passwort-Manager und bevorzugen Sie Authenticator Apps vor SMS-Codes.
- Geben Sie unter keinen Umständen ihr Passwort weiter.
- Prüfen Sie auf Seiten wie ibarry.ch, ob Ihre Zugangsdaten schon einmal in einer Datensammlung aufgetaucht sind. Falls ja, ändern Sie unbedingt Ihr Passwort.

Social Engineering

Social Engineering-Angriffe nutzen grundsätzlich die menschlichen Emotionen aus. Die Angreifer können die Hilfsbereitschaft oder Neugierde ihrer Opfer gegen sie verwenden, um sie in ihre Falle zu locken. Auch können sie ihren Opfern durch Drohungen oder der vermeintlichen Dringlichkeit ihres Anliegens Angst einflössen und sie so manipulieren. Sehr oft missbrauchen die Angreifer aber einfach das menschliche Vertrauen ihrer Opfer, um beispielsweise an vertrauliche Daten zu gelangen. Social Engineering kann im direkten Gespräch sowie auch online und am Telefon angewendet werden.

Folgende Beispielszenarien sollen Ihnen helfen, auf gewisse Muster aufmerksam zu werden:
Ihr Gesprächspartner

- befragt Sie beiläufig nach vertraulichen Informationen,
- gibt sich als Mitarbeiter aus und fordert Zugang zu einem geschützten Bereich,
- weist auf eine hohe Dringlichkeit des Anliegens hin und verwendet Drohungen,
- fordert Sie auf, Regelungen ausnahmsweise zu umgehen.

Falls Sie Opfer eines solchen Angriffs werden oder vermuten, gerade Opfer eines Angriffs zu werden, empfehlen wir folgendes Vorgehen:

- Bleiben Sie ruhig.
- Geben Sie keine Informationen weiter, sofern Sie sich nicht sicher sind, mit wem Sie sich unterhalten und welche Informationen diese Person über Sie und Ihr Unternehmen wissen darf.
- Verlangen Sie bei Anfragen den Mitarbeiter- oder Besucherausweis und lassen Sie niemals eine unbekannte Person in einen geschützten Bereich.
- Stellen Sie selbst Fragen (zum Beispiel zur Identifikation) und wiederholen Sie diese nötigenfalls. Dies blockt einerseits die konstante Befragung des Gegenübers ab, andererseits hilft es Ihnen, die Situation zu verstehen. Erfolgt der Angriff per Telefon, fragen Sie nach einer konkreten Nummer, um zurückzurufen (Anrufe dieser Art erfolgen oft mittels unterdrückter beziehungsweise anonymer Nummer) oder beenden Sie das Gespräch ohne Angabe von Informationen.
- Behalten Sie im Hinterkopf, dass Sie den «Social Engineer» nicht sofort vertreiben, sondern identifizieren wollen. So können Sie ihn von möglichen zukünftigen Angriffsversuchen auf Sie und Ihre Mitarbeitenden abhalten.

Tipps

- Achten Sie darauf, was sie auf Sozialen Medien von sich preisgeben. Nicht nur Freunde und Bekannte können dies sehen.
- Künstliche Intelligenz wird heute eingesetzt, um Sie über verschiedene Kanäle noch besser zu täuschen.
- Kontaktieren Sie bei Unsicherheit die vermeintliche Person auf einem anderen Kanal, den sie schon besitzen.

Phishing

Betreff: Rückerstattung für unbeabsichtigte Doppelzahlung - Swisscom

SS Supportteam Swisscom <kundenservice.noreply-swisscom@451c19f9e3.nxcli.io>
An: Fera, Davide

Swisscom Trust Services AG

swisscom

Sehr geehrter Kunde,

Wir bedauern zutiefst, dass Sie Ihre Rechnung doppelt bezahlt haben. Umgehend haben wir Maßnahmen ergriffen, um Ihnen eine schnelle Lösung anzubieten und sicherzustellen, dass Ihre Erfahrung mit Swisscom stets positiv bleibt.

Deshalb haben wir einen einfachen und unkomplizierten Prozess eingerichtet, um eine Rückerstattung für die überbezahlte Rechnung vom Januar 2024 zu beantragen. Klicken Sie auf den untenstehenden Button, um Ihre Rückerstattung zu erhalt

Rückerstattung beantragen

Vielen Dank für Ihr Vertrauen in Swisscom. Wir stehen Ihnen bei Fragen jederzeit zur Verfügung.

Mit freundlichen Grüßen,
Swisscom

Wenn Sie in Zukunft keine Marketing-E-Mails mehr von uns erhalten möchten, können Sie sich jederzeit abmelden. Besuchen Sie unsere Webseite, um mehr über unsere Datenschutzrichtlinie und Nutzungsbedingung

Phishing ist eine Form des Social Engineerings. Dabei wird versucht, das Vertrauen des Empfängers zu erschleichen, ihm vertrauliche Informationen zu entlocken oder sie zu Handlungen zu bewegen, um das Unternehmen zu schädigen. Phishing ist eines der grössten Einfallstore für Cyber-Angriffe.

Anhand der oben abgebildeten E-Mail wird erklärt, woran man eine Phishing-Mail erkennen kann und wie man mit dieser umgeht.

Erkennungsmerkmale (rot markierte Stellen) von oben nach unten:

1. Der angegebene Absender hat keine richtige Swisscom Absenderadresse.
2. Unpersönliche Ansprache ohne Namen. Im Normalfall wird man persönlich angesprochen, wenn man als Kunde bekannt ist.
3. Die Rechtschreibung weicht von den üblichen Regeln ab.
4. Link weist, wie die E-Mail-Adresse, keinen Bezug zu Swisscom auf.

Weitere typische Merkmale von Phishing-Mails können sein:

- landesunübliche Sprache (beispielsweise Englisch, obwohl der Service auf Deutsch verwendet wird),
- unterschiedliche Formatierungen oder Logos in der E-Mail,
- Mails an die geschäftliche Adresse, obwohl der Absender nur im privaten Umfeld genutzt wird.

Wie umgehen mit Phishing-Mails?
Nicht alle Phishing-Mails sind immer einfach erkennbar. Sollte der Verdacht bestehen, dass es sich bei einer empfangenen E-Mail um eine Phishing-Mail handelt, sollten keine Anhänge geöffnet oder Links in der E-Mail angeklickt werden.

Nicht direkt über «Antworten» auf die E-Mail antworten. Wurde die E-Mail von einer unpersönlichen Firmenadresse, zum Beispiel Support oder Kundenservice, versendet, kontaktieren Sie das Unternehmen über einen unabhängig verifizierten Kanal. Gehen Sie beispielsweise direkt über den Internet-Browser auf die Firmen-Seite und schauen Sie dort nach Kontaktmöglichkeiten.
Wenn Sie eine IT-Abteilung haben, kontaktieren Sie dort die Kollegen, um die E-Mail zu melden und gegebenenfalls weitere Mitarbeitende zu warnen.

Wie kann ich mich schützen?
Verwenden Sie für jeden Login ein unterschiedliches Passwort. Wenn immer angeboten, aktivieren Sie eine Multi-Faktor-Authentifizierung. Diese bietet einen zusätzlichen Schutz und verringert das Risiko eines Missbrauchs. Keine Bank wird sie jemals per E-Mail auffordern, ein Passwort zu ändern oder Kreditkartendaten zu verifizieren.

Tipps

- Phishing gibt es nicht nur per E-Mail, sondern auch über SMS (Smishing), Telefonanrufe (Vishing) und QR-Codes (Quishing).
- Im Zweifelsfall kontaktieren Sie das Kundencenter des Absenders telefonisch oder per E-Mail.
- Fragen Sie sich, ob Sie diese Nachricht erwartet haben.

Ransomware

Diese Bezeichnung ist zusammengesetzt aus dem Englischen «ransom» für Lösegeld und «malware» für Schadsoftware. Dabei handelt es sich um Schadprogramme, auch Erpressungs- oder Krypto-Trojaner genannt. Ziel der Kriminellen ist es, Lösegeld zu erpressen. Dies wird entweder dadurch erreicht, dass die Daten im Netzwerk verschlüsselt werden oder durch den Diebstahl der Daten vor der Verschlüsselung, indem die Daten zu einem externen Server der Kriminellen gesendet werden. Im Anschluss wird ein Lösegeld erpresst, entweder für die Entschlüsselung der Daten oder die Nichtveröffentlichung der Daten.

Wie funktioniert ein Ransomware-Angriff?
Es gibt verschiedene Einfallstore für einen Ransomware-Angriff. Am verbreitetsten ist immer noch der klassische Weg über eine Phishing-E-Mail. Sensibilisieren Sie ihre Mitarbeitenden über die Risiken und achten Sie beim Umgang mit E-Mails insbesondere darauf, nicht unbedacht auf Links zu klicken oder Anhänge zu öffnen. Es könnte dazu führen, dass die Ransomware in das Unternehmensnetzwerk gelangt, sich dort ausbreitet und einen möglichst grossen Schaden verursacht.

Ein weiteres Einfallstor sind Systeme mit Schwachstellen, das heisst mit fehlenden Sicherheits-Updates, beispielsweise Betriebssysteme oder Web-Browser.
Der dritte weitverbreitete Weg sind exponierte Fernwartungszugänge, die direkt über das Internet erreichbar sind.

Wie kann ich mich und mein Unternehmen schützen?
Mit präventiven Massnahmen kann man das Risiko erheblich reduzieren:

- Installieren Sie Sicherheits-Updates zeitnah nach Erscheinen.
- Setzen Sie nur Software ein, welche vom Anbieter noch unterstützt wird.
- Erstellen Sie möglichst automatisiert regelmässige Backups und lagern Sie diese ausserhalb ihres Netzwerks.
- Testen Sie regelmässig, ob die Backups funktionsfähig sind und führen Sie Wiederherstellungstests durch.
- Bei der Wahl des Backups bedenken Sie, wie viel Zeit die vollständige Wiederherstellung in Anspruch nimmt und wie viel Datenverlust für ihr Unternehmen akzeptabel ist.
- Sensibilisieren Sie Mitarbeitende, wie im Falle eines Vorfalls vorzugehen ist und wie verdächtige E-Mails oder ungewöhnliche Vorkommnisse zu melden sind.

Was tun bei einem Vorfall?
Ruhe bewahren. Meist ist es hilfreich, externe Spezialisten hinzuzuziehen, die Erfahrung mit Cyberangriffen haben. Diese können Sie beraten und Ihnen dabei helfen zu identifizieren, wie es zu dem Vorfall gekommen ist und welche Schritte sinnvoll sind, um möglichst schnell wieder arbeiten zu können.

Kontaktieren Sie das Bundesamt für Cybersicherheit (BACS). Die dortigen Spezialisten unterstützen mit hilfreichen Informationen bei der Analyse und dem Vorgehen.

Tipps

- Setzen Sie nur Software ein, die vom Anbieter noch unterstützt wird.
- Erstellen Sie einen Plan für den Fall eines Cyberangriffs.
- Installieren Sie auf allen Geräten eine Endpoint-Protection-Software, um Angriffe frühzeitig zu erkennen.

Weitere wichtige präventive Richtlinien

Vorbereitungen treffen
Informationssicherheit ist eine Herausforderung für jedes Unternehmen. Bereiten Sie sich im Vorfeld auf einen Cyberangriff vor. Erstellen Sie einen Plan und trainieren Sie, was im Falle eines Vorfalls zu tun ist. Im Falle eines Cyberangriffs ist es zu spät, sich darüber Gedanken zu machen.

Daten sichern – Backups erstellen und regelmässig testen
Nicht nur im Falle eines Cyber-Angriffs können sensible Daten wie Kundeninformationen oder Daten verloren gehen. Auch andere Ereignisse wie Feuer oder Wasserschäden können zu Datenverlust führen. Erstellen Sie deshalb regelmässig Sicherheitskopien – sogenannte «Backups» – von Ihren Daten. Wichtig ist auch, regelmässig zu testen, ob sich die gesicherten Daten wiederherstellen lassen. Lagern Sie die Backups getrennt von den Ursprungsdaten, damit diese im Ereignisfall auch verfügbar sind. Bei der Erstellung des Backups überlegen Sie sich im Vorfeld, wie viel Datenverlust für sie akzeptabel ist. Abhängig davon sollten sie die Backup-Zyklen planen.

Updates
Installieren Sie zeitnah verfügbare Sicherheitsupdates für Ihre Betriebssysteme und Programme. Achten Sie darauf, dass die eingesetzte Software vom Anbieter noch unterstützt wird.

Gesunder Menschenverstand
Lassen Sie beim Surfen und bei sensitiven Internetgeschäften immer den gesunden Menschenverstand walten. Lassen Sie sich nicht durch eine E-Mail oder einen Anruf unter Druck setzen. Es ist immer Zeit zum Nachdenken da.

Staatliche Unterstützung
Das Bundesamt für Cybersicherheit (BACS) bietet Informationen und Hilfestellung zu aktuellen Gefahren und Massnahmen sowie auch ein Meldeformular bei Vorfällen für Unternehmen und Privatpersonen an.

Wie kann ich prüfen, ob ich oder meine Daten betroffen sind?
iBarry ist die Schweizer Plattform für Internetsicherheit. Die Seite bietet hilfreiche Informationen und Tools für jedes Unternehmen, um die eigenen Mitarbeitenden zu sensibilisieren.

Die Seite stellt auch einen Sicherheitscheck zur Verfügung, bei dem man überprüfen kann, ob die eigenen Zugangsdaten bei Webdiensten gestohlen wurden.

Tipps
- **Staatliche Unterstützung beim Bundesamt für Cybersicherheit (https://www.ncsc.admin.ch/)**
- **iBarry - Plattform für Internetsicherheit (https://www.iBarry.ch)**

Baloise Group
Aeschengraben 21
CH-4002 Basel
baloise.com
www.baloise.com/digital-scouts

000.1038d 4.24 pdf